ON WHITEHEAD'S FIRST FREE-GROUP ALGORITHM, CUTVERTICES, AND FREE-PRODUCT FACTORIZATIONS

WARREN DICKS*

ABSTRACT. Let F be any finite-rank free group, and R be any finite subset of $\{g, [g] : g \in F - \{1\}\}$, where $[g] := \{fgf^{-1} : f \in F\}$. By an R-allocating F-factorization we mean a set $\mathcal{H}$ of nontrivial subgroups of F such that $\underset{H \in \mathcal{H}}{*} H = F$ and $R \subseteq \{h, [h] : h \in H, H \in \mathcal{H}\}$. We show that Whitehead's (fast) cutvertex algorithm inputs the pair (F, R) and outputs a maximum-size R-allocating F-factorization. Richard Stong showed this in the case where $R \subseteq F$ or $R \subseteq \{[g] : g \in F\}$, thereby unifying and generalizing a collection of results obtained by Berge, Bestvina, Lyon, Shenitzer, Stallings, Starr, and Whitehead. Our proof is based on the interaction between two normal forms for the elements of F, rather than the algebraic topology of handlebodies, trees, or graph folding.

1. OUTLINE

Throughout this article, let F be any finite-rank free group, X be any F-basis, and R be any finite set that consists of nontrivial F-elements and nontrivial F-classes. (An F-*basis* is a free-generating set for F, an F-*element* is an element of F, and a (nontrivial) F-*class* is the conjugacy class of a (nontrivial) F-element.)

For $f, g \in F$ and $B \subseteq F$, we write ${}^{f}g := fgf^{-1}$, ${}^{F}g := \{{}^{h}g : h \in F\}$, and ${}^{\{F\}}B := \{{}^{F}b : b \in B\}$.

Suppose that $\mathcal{H}$ is a multiset of subgroups of F such that the induced map $\underset{H \in \mathcal{H}}{*} H \to F$ is an isomorphism. Here, we say that $\mathcal{H}$ is an F-*factorization*, and call the elements of $\mathcal{H}$ *the factors*. Sometimes we also say that the expression $\underset{H \in \mathcal{H}}{*} H$ is an F-factorization. We say that the F-factorization $\mathcal{H}$ is R-*allocating* if each element of $\mathcal{H}$ is nontrivial and $R \subseteq \{h, {}^{F}h : h \in H, H \in \mathcal{H}\}$. If, moreover, no proper free-product refinement of $\underset{H \in \mathcal{H}}{*} H$ is R-allocating, we say that the R-allocating F-factorization $\mathcal{H}$ is *atomic*. Since F has finite rank, atomic R-allocating F-factorizations exist, and we want to be able to find one as quickly as possible.

In §2, we review the earlier results on this topic, starting with Whitehead's cutvertex lemma.

In §3, we show that atomic R-allocating F-factorizations are all as similar to each other as may reasonably be expected. When $R \subseteq F$, each atomic R-allocating F-factorization gives the unique inclusion-smallest free-product factor of F which includes R; this is the only information it gives when $|R| = 1$, where we may as well assume that $R \subseteq F$.

In §4, we give a careful treatment of concepts introduced by Whitehead(1936-01, §2). We denote by $\mathcal{P}(X; R)$ the finest partition of X that respects the X-support of each element of R, which means that the F-factorization $\underset{Y \in \mathcal{P}(X;R)}{*} \langle Y \rangle$ is R-allocating; this appeared in work of Hoare & Karrass & Solitar(1971, §2) with different notation and terminology. Using $\mathcal{P}(X; R)$ and Whitehead's graphs, we define R-*cutvertex-free* F-bases. We then present *Whitehead's cutvertex algorithm*, §4.6 below, which inputs the pair (X, R) and outputs an R-cutvertex-free F-basis. (By an *algorithm* we mean a procedure with choices whose possible outputs have some specified property.)

In §5, we present *the general cutvertex lemma*, §5.2 below, which says

(1) if X is R-cutvertex-free, then the R-allocating F-factorization $\underset{Y \in \mathcal{P}(X;R)}{*} \langle Y \rangle$ is atomic.

In summary, we show that Whitehead's (fast) cutvertex algorithm inputs the pair (X, R) and outputs an atomic R-allocating F-factorization.

---

2. Chronology of proofs of cases of the general cutvertex lemma

• Whitehead(1936-01) proved the case of (1) where R is a subset of B or ${}^{\{F\}}B$ for some F-basis B; in detail, he used the algebraic topology of a certain three-manifold to prove that if X is R-cutvertex-free here, then R is a subset of $X \cup X^{-1}$ or ${}^{\{F\}}(X \cup X^{-1})$ respectively. This is called *Whitehead's cutvertex lemma*, §5.3 below. Gersten(1984, Example) announced that graph-theoretic machinery he had developed could be used to prove the $R \subseteq X \cup X^{-1}$ result, and Hoare(1988, Theorem 3) provided such a proof.

Put together, Whitehead's cutvertex algorithm and cutvertex lemma constituted the first-ever *sub-basis algorithm*, by which we mean an algorithm which extends a given finite subset of F to an F-basis or determines that that is not possible, and analogously for a given finite set of F-classes.

• Shenitzer(1955, Corollary) used another result of Whitehead(1936-10, Theorem 3) to prove the case of (1) where $|R| = 1$ and X is R-minimizing; the latter concept is defined in §5.4 below.

• Lyon(1980, Theorem 1) developed Shenitzer's method to prove the case of (1) where R is a subset of F or ${}^{\{F\}}F$ and X is R-minimizing.

• Starr(1992) gave cutvertex arguments which, in the form distilled by Wu(1996, §1), and in the light of a result of Lyon(1980, Theorem 2), prove what is the case of (1) where R is the set of F-classes determined by a finite set of disjoint simple closed curves on the boundary of a handlebody which has F as fundamental group. It was Stallings(1999, §3) who realized that Whitehead's cutvertex algorithm was being given a completely new application here.

• John Berge, in a 1993 preprint, proved the case of (1) where $|R| = 1$, by using the algebraic topology of Whitehead's three-manifold; see Stallings(1999, Corollary 2.5). Nataša Macura kindly informed me that Mladen Bestvina independently proved the same case, by analyzing infinite paths in a Cayley tree; see Martin(1995, Theorem 49).

• Stong(1997, Theorem 3) proved the case of (1) where $R \subseteq {}^{\{F\}}F$, by analyzing bi-infinite paths in a Cayley tree. Independently, Stallings(1999, Theorem 2.4) proved the same case, by using the algebraic topology of Whitehead's three-manifold. An elegant graph-theoretic folding proof was given by Wilton(2018, Lemma 2.10) and, independently, by Heusener & Weidmann(2019, §3).

• Stong(1997, Theorem 10) proved the case of (1) where $R \subseteq F$, by using the algebraic topology of a handlebody. A Bass-Serre-theoretic two-tree proof was given by Dicks(2014, §2).

3. Atomic R-allocating F-factorizations

Recall that F is a finite-rank free group and R is a finite subset of $\left\{ g, {}^{F}g : g \in F - \{1\} \right\}$.

3.1. **Definitions.** Artin(1926) gave the normal form for an element of a free product of groups, as presented by Serre(1977, I.1.2.1). This may be used to prove that if $\mathcal{H}$ is any F-factorization, then, for any $H_1, H_2 \in \mathcal{H}$ and $g_1, g_2 \in F$, if ${}^{g_1}H_1 \cap {}^{g_2}H_2 \neq \{1\}$ in F, then $g_1H_1 = g_2H_2$ in F, and $H_1 = H_2$ in $\mathcal{H}$ and in F. This implication may also be viewed as a consequence of the result of Serre(1977, I.5.3.12) that if $\mathcal{H} \neq \emptyset$, then the disjoint union of the left F-sets F/H, $H \in \mathcal{H}$, is the vertex-set of a left F-tree with trivial edge stabilizers.

Recall that an F-factorization $\mathcal{H}$ is said to be R-allocating if each element of $\mathcal{H}$ is nontrivial, each F-element $r \in R$ is an element of some $H \in \mathcal{H}$, and each F-class $r \in R$ contains an element of some $H \in \mathcal{H}$, which implies that $r \cap H$ is an H-class; in each case, we now see that the element H of $\mathcal{H}$ is uniquely determined by r, and we shall say that *r is allocated to the factor H*. For each $H \in \mathcal{H}$, we write $R_{|H,\mathcal{H}}$ to denote the set of elements of R which are allocated to H, sometimes viewed as a set of H-elements and H-classes. Notice that $\{R_{|H,\mathcal{H}} : H \in \mathcal{H}\} - \{\emptyset\}$ is a partition of R.

If $F = \{1\}$, then $R = \emptyset$, and $\emptyset$ is the unique R-allocating F-factorization. If $F \neq \{1\}$, then $\{F\}$ is an R-allocating F-factorization; if it is the only one, then we say that F is an R-*atom*. Thus, an R-allocating F-factorization $\mathcal{H}$ is atomic if and only each $H \in \mathcal{H}$ is an $R_{|H,\mathcal{H}}$-atom. □

3.2. **Proposition.** *All the atomic R-allocating F-factorizations have the same number of factors. They all induce the same partition of R. For each $r \in R$, they all have the same F-conjugacy orbit of the factor to which r is allocated, and if r is an F-element, they all have the same factor to which r is allocated. All the factors with no elements of R allocated to them are free subgroups of rank one.*

Proof. Consider any two atomic R-allocating F-factorizations $\mathcal{H}$ and $\mathcal{K}$, and any $H \in \mathcal{H}$. The subgroup theorem of Kurosch(1934) gives an H-factorization $H_0 * \underset{K \in \mathcal{K}}{*} \underset{a \in A_{H,K}}{*} (H \cap {}^{a}K)$ where H_0 is a free group

and, for each $K \in \mathcal{K}$, $A_{H,K}$ is a certain subset of F such that $1 \in A_{H,K}$ and the map $A_{H,K} \to H\backslash F/K$, $a \mapsto H{\cdot}a{\cdot}K$, is bijective; see, for example, Serre(1977, I.5.5.14). Kurosch's theorem may be used to prove the result of Nielsen(1921) that H is a free group.

Consider any $r \in R_{|H,\mathcal{H}}$. There exists a (necessarily unique) $K \in \mathcal{K}$ such that if r is an F-element, then $r \in H$ and $r \in K$, while if r is an F-class, then r contains an H-element h and a K-element k. In the former event, $r \in H \cap {}^1K$. In the latter event, since r is an F-class, $h = {}^gk$ for some $g \in F$, and then $g = h'{\cdot}a{\cdot}k'$ for some $(h', a, k') \in H \times A_{H,K} \times K$, and then r contains ${}^{h'^{-1}}h = {}^{a{\cdot}k'}k \in H \cap {}^aK$. Thus, we obtain an $R_{|H,\mathcal{H}}$-allocating H-factorization from $H_0 * \underset{K\in\mathcal{K}}{*} \underset{a\in A_{H,K}}{*} (H \cap {}^aK)$ by omitting all the trivial factors.

Since $\mathcal{H}$ is an atomic R-allocating F-factorization, H is an $R_{|H,\mathcal{H}}$-atom, and there are three possibilities. If $R_{|H,\mathcal{H}} = \emptyset$, then the rank of H is 1. If $R_{|H,\mathcal{H}}$ contains an H-element, then $H = H \cap K$ and $R_{|H,\mathcal{H}} \subseteq R_{|K,\mathcal{K}}$; by symmetry, $K = K \cap H = H$ and $R_{|H,\mathcal{H}} = R_{|K,\mathcal{K}}$. If $R_{|H,\mathcal{H}}$ is nonempty and consists of H-classes, then $H = H \cap {}^aK$ and $R_{|H,\mathcal{H}} \subseteq R_{|K,\mathcal{K}}$; by symmetry, K is also included in an F-conjugate of H, and we see that $H = {}^aK$ and $R_{|H,\mathcal{H}} = R_{|K,\mathcal{K}}$. The result now follows. $\qquad\square$

3.3. Corollary (Stong). *If R is a subset of B or ${}^{\{F\}}B$ for some F-basis B, then each atomic R-allocating F-factorization equals $\underset{x \in X}{*} \langle x \rangle$ for some F-basis X such that R is a subset of X or ${}^{\{F\}}X$ respectively.* $\qquad\square$

4. Whitehead's cutvertex algorithm

Recall that F is a finite-rank free group, X is an F-basis, and R is a finite subset of $\{g, {}^Fg : g \in F-\{1\}\}$.

4.1. Notation. We write $X^{\pm 1} := X \cup X^{-1}$ and $X^{0,\pm 1} := \{1\} \cup X^{\pm 1}$.

If r is any F-element (resp. nontrivial F-class), then by an $X^{\pm 1}$-*word for* r we mean any finite sequence $(x_1, x_2, \ldots, x_n)$ of elements of $X^{\pm 1}$ such that r equals (resp. contains) the product $x_1 x_2 \cdots x_n$; here, we set $x_0 := 1$ (resp. $x_0 := x_n$) and $x_{n+1} := 1$ (resp. $x_{n+1} := x_1$). There exists some $X^{\pm 1}$-word $(x_1, x_2, \ldots, x_n)$ for r such that $x_i^{-1} \neq x_{i+1}$ for each $i \in \{0, 1, 2, \ldots, n\}$, and such a word is unique (resp. unique up to cyclic permutation), which allows us to define

$$X\text{-length}(r):=n, \quad X\text{-turns}(r):=\big\{(x_0^{-1}, x_1), (x_1^{-1}, x_2), \ldots, (x_n^{-1}, x_{n+1})\big\}, \quad X\text{-support}(r):=\{x_1, x_2, \ldots, x_n\}^{\pm 1}\cap X.$$

We call each element of X-turns(r) an X-*turn of* r. If r is the trivial F-class, we define X-length$(r):=0$, X-turns$(r) := \emptyset$, and X-support$(r):=\emptyset$. It is not difficult to see that if r is any F-class, then, for each $g \in r$, X-turns$(r) \subseteq X$-turns(g^2).

Let R' be any subset of $F \cup {}^{\{F\}}F$. We write

$$X\text{-length}(R') := \sum_{r \in R'} X\text{-length}(r) \in \{\infty, 0, 1, 2, \ldots\} \quad \text{and} \quad X\text{-turns}(R') := \bigcup_{r \in R'} X\text{-turns}(r) \subseteq X^{0,\pm 1}\times X^{0,\pm 1}.$$

We call each element of X-turns(R') an X-*turn of* R'. We denote by $\mathcal{P}(X; R')$ the finest partition of X such that, for each $r \in R'$, some element of the partition includes X-support(r). We define an operation which takes a set of subsets of X with two overlapping elements and replaces those two subsets with their union, thereby reducing the number of subsets; if we start with the (finite) set $\{X\text{-support}(r) : r \in R'\} \cup \{\{x\} : x \in X\}$ and apply this operation as often as possible, then we obtain $\mathcal{P}(X; R')$. $\qquad\square$

4.2. Definitions. For any set V and any element (v, w) of $V \times V$, we say that (v, w) *meets* each subset of V which contains v or w; we say also that (v, w) *meets* v and w.

By a *graph* Γ, we mean a set V together with a subset E of $V \times V$. Then V is called the *vertex-set* of Γ, denoted VΓ, and its elements are called Γ-*vertices*, while E is called the *edge-set* of Γ, denoted EΓ, and its elements are called Γ-*edges*. A Γ-vertex $v_\dagger$ is said to be a *cutvertex of* Γ (*in the sense of Whitehead*) if V$\Gamma - \{v_\dagger\}$ equals the union of two disjoint nonempty subsets V_1 and V_2 such that $V_1 \overset{\Gamma}{\not\leftrightarrow} V_2$, where this symbol means "no Γ-edge meets both V_1 and V_2". We shall use corresponding depictions of related phrases.

We let $\mathbb{W}(X, R)$ denote the graph whose vertices are those elements of $X^{0,\pm 1}$ which are met by some X-turn of R and whose edges are the X-turns of R. A cutvertex of $\mathbb{W}(X, R)$ is called an X-*cutvertex of* $\mathbb{W}(X, R)$ if it lies in $X^{\pm 1}$, that is, it does not equal 1.

For each $Y \in \mathcal{P}(X; R)$, we set $R_{|Y,X} := \{r \in R : X\text{-support}(r) \subseteq Y\}$; then $\{R_{|Y,X} : Y \in \mathcal{P}(X; R)\} - \{\emptyset\}$ is a partition of R. We sometimes view the elements of $R_{|Y,X}$ as $\langle Y \rangle$-elements and $\langle Y \rangle$-classes; here, $\mathcal{P}(Y; R_{|Y,X}) = \{Y\}$. We say X is R-*cutvertex-free* if, for each $Y \in \mathcal{P}(X; R)$, $\mathbb{W}(Y, R_{|Y,X})$ has no Y-cutvertices.

An F-basis X' is a *Whitehead neighbour* of X if $X' \subseteq \{1, y^{-1}\}{\cdot}X{\cdot}\{1, y\}$ for some $y \in (X \cap X')^{\pm 1}$. $\qquad\square$

4.3. Examples. If $X = \{x, y\}$ and $R = \{x, {}^F y\}$, then $\mathbb{EW}(X, R) = \{(x^{-1}, 1), (1, x), (y^{-1}, y)\}$ and $\mathbb{W}(X, R)$ has four X-cutvertices. Here, $\mathcal{P}(X; R) = \{\{x\}, \{y\}\}$, and X is R-cutvertex-free.

If $X = \{x, y\}$ and $R = \{x^2 y x^{-1} y^{-1}\}$, then $\mathbb{EW}(X, R) = \{(1, x), (x, y^{-1}), (y^{-1}, x^{-1}), (x^{-1}, y), (y, 1), (x^{-1}, x)\}$ and $\mathbb{W}(X, R)$ has no cutvertices. Here, $\mathcal{P}(X; R) = \{X\}$, and X is R-cutvertex-free. □

4.4. Remarks. In $\mathbb{W}(X, R)$, each vertex is met by some edge; each edge meets two vertices since $1 \notin R$; $\mathrm{V}\mathbb{W}(X, R) = \emptyset$ if and only if $R = \emptyset$; and $1 \in \mathrm{V}\mathbb{W}(X, R)$ if and only if R contains some F-element.

By partitioning X manually, we reduce our study to the case where $\mathcal{P}(X; R) = \{X\}$. With the exception of the famous final phrase in the statement of Whitehead's cutvertex lemma, §5.3 below, we shall work with $\mathbb{W}(X, R)$ only in the case where $\mathcal{P}(X; R) = \{X\}$. One consequence is that connectivity is not mentioned in our arguments.

Suppose that $\mathcal{P}(X; R) = \{X\}$. Here, $X \neq \emptyset$. If $R = \emptyset$, then $|X| = 1$ and $\mathrm{V}\mathbb{W}(X, R) = \emptyset$. If $R \neq \emptyset$, then $X^{\pm 1} \subseteq \mathrm{V}\mathbb{W}(X, R) \subseteq X^{0, \pm 1}$. If $\mathbb{W}(X, R)$ *has* an X-cutvertex, then Subroutine 4.5 below constructs a Whitehead neighbour X' of X such that X'-length$(R) < X$-length(R). If $\mathbb{W}(X, R)$ has *no* X-cutvertices, then Theorem 5.1 below says that F is an R-atom (Gr. $\check{\alpha}\tau o\mu$-$o\varsigma$ 'no cut'). □

Whitehead, Stong, Stallings, and others gave cases of the following, using similar ideas.

4.5. Subroutine. *When $\mathcal{P}(X; R) = \{X\}$ and $\mathbb{W}(X, R)$ has an X-cutvertex, the following three-step procedure outputs a Whitehead neighbour X' of X such that X'-length$(R) < X$-length(R).*

Step 1. *We set $\Gamma := \mathbb{W}(X, R)$. We shall see that $X^{\pm 1} \subseteq \mathrm{V}\Gamma \subseteq X^{0, \pm 1}$. We shall find a $y_\dagger \in X^{\pm 1}$ and an expression of $\mathrm{V}\Gamma - \{y_\dagger\}$ as the union of two disjoint subsets Y_- and Y_+ such that $y_\dagger^{-1} \in Y_- \overset{\Gamma}{\not\leftrightarrow} Y_+ \overset{\Gamma}{\leftrightarrow} y_\dagger$.*

Here, $X^{\pm 1} \subseteq \mathrm{V}\Gamma \subseteq X^{0, \pm 1}$ since $\mathcal{P}(X; R) = \{X\}$ and $\mathrm{V}\Gamma \neq \emptyset$. Since Γ has an X-cutvertex, we may find some $x_\dagger \in X^{\pm 1}$ and express $\mathrm{V}\Gamma - \{x_\dagger\}$ as the union of two disjoint nonempty subsets X_- and X_+ such that $x_\dagger^{-1} \in X_- \overset{\Gamma}{\not\leftrightarrow} X_+$. If $X_+ \overset{\Gamma}{\leftrightarrow} x_\dagger$, then setting $y_\dagger := x_\dagger$, $Y_- := X_-$, and $Y_+ := X_+$ gives the desired result; thus, we may assume that $X_+ \overset{\Gamma}{\not\leftrightarrow} x_\dagger$. Here, $\mathrm{V}\Gamma$ equals the union of two disjoint nonempty subsets $Y_- := X_- \cup \{x_\dagger\}$ and X_+ such that $Y_- \overset{\Gamma}{\not\leftrightarrow} X_+$. For each $v \in X_+$, $v \overset{\Gamma}{\leftrightarrow} X_+ - \{v\}$; in particular, $X_+ \neq \{1\}$. Since $\mathcal{P}(X; R) = \{X\}$, the set $\{\langle X_+ \rangle, \langle Y_- \rangle\}$ is not an R-allocating F-factorization induced by a partition of X, which means that there exists some $y_\dagger \in X_+$ such that $y_\dagger^{-1} \in Y_-$. Now $\mathrm{V}\Gamma - \{y_\dagger\}$ equals the union of two disjoint subsets Y_- and $Y_+ := X_+ - \{y_\dagger\}$ such that $y_\dagger^{-1} \in Y_- \overset{\Gamma}{\not\leftrightarrow} Y_+ \overset{\Gamma}{\leftrightarrow} y_\dagger$. Step 1 is completed. We have no further need of the two original hypotheses.

Step 2. *We have found $y_\dagger \in X^{\pm 1}$, and we shall construct an $\ell \in \{-1, 0\}$ and a map $\chi : X^{0, \pm 1} \to \{\ell, \ell+1\}$, $v \mapsto \chi(v)$, such that the following hold: $\chi(1) = 0$; $\chi(y_\dagger) = \chi(y_\dagger^{-1}) = \ell$; at least one X-turn (v, w) of R is χ-cut in the sense that $\chi(v) \neq \chi(w)$; and every χ-cut X-turn of R meets $y_\dagger$.*

We set $\ell := -|\{1\} \cap Y_+|$, and form the map χ which carries $\{1\}$ to $\{0\}$, $Y_- \cup \{y_\dagger\}$ to $\{\ell\}$, and Y_+ to $\{\ell+1\}$; our choice of ℓ ensures that χ is well-defined. The χ-cut X-turns of R are then the Γ-edges which meet $y_\dagger$ and Y_+, of which there exists at least one. Step 2 is completed. We have no further need of Step 1.

Step 3. *We shall construct a Whitehead neighbour X' of X such that X'-length$(R) < X$-length(R).*

We set $x' := y_\dagger^{-\chi(x)} \cdot x \cdot y_\dagger^{\chi(x^{-1})}$ for each $x \in X^{\pm 1}$, and set $X' := \{x' : x \in X\}$. Then $(x')^{-1} = (x^{-1})'$, $y_\dagger' = y_\dagger$, and X' is a Whitehead neighbour of X. We consider an arbitrary $r \in R$, and let $(x_1, x_2, \ldots, x_n)$ be a shortest possible $X^{\pm 1}$-word for r. Then $n \geqslant 1$. If r is an F-element, we set $x_0 := x_{n+1} := 1$; if r is an F-class, we set $x_0 := x_n$ and $x_{n+1} := x_1$. For each $i \in \{0, 1, \ldots, n\}$, (x_i^{-1}, x_{i+1}) is an X-turn of r, and we let k_i denote the unique element of the subset $\chi(\{x_i^{-1}, x_{i+1}\} - \{y_\dagger\})$ of $\{\ell, \ell+1\}$. For each $i \in \{1, 2, \ldots, n\}$, we set $g_i := y_\dagger^{-k_{i-1}} x_i y_\dagger^{k_i}$, and we then have the following trichotomy:

    Possibility 1: $x_i = y_\dagger$ and (x_{i-1}^{-1}, x_i) is χ-cut; equivalently, $k_{i-1} \neq \chi(x_i)$.

        Here $k_i = \chi(x_i^{-1})$ since $x_i^{-1} \neq y_\dagger$, and then $g_i = y_\dagger^{-k_{i-1}} x_i y_\dagger^{k_i} = y_\dagger^{-(\ell+1)+(1)+(\ell)} = 1$.

    Possibility 2: $x_i = y_\dagger^{-1}$ and (x_i^{-1}, x_{i+1}) is χ-cut; equivalently, $k_i \neq \chi(x_i^{-1})$.

        Here $k_{i-1} = \chi(x_i)$ since $x_i \neq y_\dagger$, and then $g_i = y_\dagger^{-k_{i-1}} x_i y_\dagger^{k_i} = y_\dagger^{-(\ell)+(-1)+(\ell+1)} = 1$.

    Possibility 3: $k_{i-1} = \chi(x_i)$ and $k_i = \chi(x_i^{-1})$.

        Here $g_i = y_\dagger^{-k_{i-1}} x_i y_\dagger^{k_i} = y_\dagger^{-\chi(x_i)} x_i y_\dagger^{\chi(x_i^{-1})} = x_i'$.

Since $n = X\text{-length}(r)$, we see that $X'\text{-length}(g_1g_2\cdots g_n) \leqslant X\text{-length}(r)$ and that if some X-turn of r is χ-cut, then $X'\text{-length}(g_1g_2\cdots g_n) < X\text{-length}(r)$. Now

$$g_1g_2\cdots g_n = (y_\dagger^{-k_0}x_1y_\dagger^{k_1})(y_\dagger^{-k_1}x_2y_\dagger^{k_2})\cdots(y_\dagger^{-k_{n-1}}x_ny_\dagger^{k_n}) = y_\dagger^{-k_0}x_1x_2\cdots x_ny_\dagger^{k_n}.$$

If r is an F-element, then $k_0 = \chi(x_0^{-1}) = \chi(1) = 0$ and $k_n = \chi(x_{n+1}) = \chi(1) = 0$; here, $g_1g_2\cdots g_n = r$. If r is an F-class, then $k_0 = k_n$; here, $g_1g_2\cdots g_n \in r$. Thus, $X'\text{-length}(r) \leqslant X'\text{-length}(g_1g_2\cdots g_n)$. Since at least one X-turn of R is χ-cut, we see that $X'\text{-length}(R) < X\text{-length}(R)$. $\qquad\square$

4.6. Whitehead's cutvertex algorithm. Given (X, R), we ask if there exists some $Y \in \mathcal{P}(X; R)$ such that $\mathbb{W}(Y, R_{|Y,X})$ has a Y-cutvertex. If yes, then Subroutine 4.5 outputs a Whitehead neighbour Y' of Y such that $Y'\text{-length}(R_{|Y,X}) < Y\text{-length}(R_{|Y,X})$, and we start anew with X replaced with its Whitehead neighbour $X' := (X-Y) \cup Y'$, for which $X'\text{-length}(R) < X\text{-length}(R)$. If no, we output X, and then stop. This algorithm eventually outputs an R-cutvertex-free F-basis, and then stops. $\qquad\square$

4.7. Notes on Whitehead's article. In the types of graphs constructed by Whitehead(1936-01,§2), each edge is given a multiplicity and each copy of the edge is divided into at least three edges by adding new vertices. It is important for his arguments that cutvertices are added to his versions of, for example, $\mathbb{W}(\{x\}, \{^Fx\})$ and $\mathbb{W}(\{x,y\}, \{x,y\})$.

In the one sentence where he dealt with connected subgraphs, Whitehead overlooked one case, and we work with $\mathcal{P}(X; R)$ largely to handle that case. Stong(1997) and, independently, Stallings(1999) handled it by working with connected subgraphs (where their term "cut vertex" conforms to standard usage). With any of these straightforward rectifications, Whitehead's argument gives a valid algorithm. $\qquad\square$

5. The general cutvertex lemma

Whitehead, Stong, Stallings, and others proved cases of the following, using mainly the algebraic topology of handlebodies; we use the interaction between two normal forms.

5.1. Theorem. *If $\mathcal{P}(X; R) = \{X\}$ and F is not an R-atom, then $\mathbb{W}(X, R)$ has an X-cutvertex.*

Proof (essentially following Dicks(2014, §2)). Set $\Gamma := \mathbb{W}(X, R)$. As $\mathcal{P}(X; R) = \{X\}$, we have $F \neq \{1\}$ and, also, if $|X| \neq 1$ then $\mathrm{V}\Gamma \supseteq X^{\pm 1}$. As F is not an R-atom and $F \neq \{1\}$, there exists some R-allocating F-factorization $H_1 * H_2$. Thus, $\mathrm{V}\Gamma \supseteq X^{\pm 1}$ since $|X| \neq 1$.

In the case where $\mathrm{V}\Gamma = X^{\pm 1}$, R consists of F-classes, hence $^aR = R$ for each $a \in F$, and, by replacing $\{H_1, H_2\}$ with a suitable $\{^aH_1, {}^aH_2\}$, we may assume that the shortest $X^{\pm 1}$-word $(y_1, y_2, \ldots, y_{n_0})$ for some element of $(H_1 \cup H_2)-\{1\}$ has $y_{n_0} \neq y_1^{-1}$. Taking $y := y_1$ and $y' := y_{n_0}^{-1}$, we have

(2) if $\mathrm{V}\Gamma \neq X^{0,\pm 1}$, then there exist X-turns $(1, y)$ and $(y', 1)$ of $H_1 \cup H_2$ with $1 \neq y \neq y' \neq 1$.

For $f \in F = H_1 * H_2$, there exists a unique finite sequence $(h_1, h_2, \ldots, h_m)$ of nontrivial elements of $H_1 \cup H_2$ such that $h_1h_2\cdots h_m = f$ and neither H_1 nor H_2 contains two consecutive terms of the sequence. Here, we set

$$\delta(f) := \left\{h_j^{-1}h_{j-1}^{-1}\cdots h_1^{-1} : j \in \{1, 2, \ldots, m-1\}\right\} \qquad \text{and} \qquad \chi(f) := \begin{cases} 1 & \text{if } f \neq 1 \text{ and } h_1 \in H_1, \\ 0 & \text{otherwise.} \end{cases}$$

Clearly,

(3) $\delta(f)$ is finite and, also, $\delta(f) = \emptyset$ if and only if $f \in H_1 \cup H_2$.

We have defined a map $\chi : F \to \{0, 1\}$, $g \mapsto \chi(g)$, and it is not difficult to use induction on m to prove that

(4) $\delta(f) = \{g \in F : g \neq 1,\ gf \neq 1,\ \text{and } \chi(g) \neq \chi(gf)\}$.

Since $\mathcal{P}(X; R) = \{X\}$, the R-allocating F-factorization $H_1 * H_2$ is not induced by a partition of X; hence, there exists some $x \in X-(H_1 \cup H_2)$, and then $\delta(x) \neq \emptyset$ by (3). Also, $X^{\pm 1}$ is finite, and, for each $x \in X^{\pm 1}$, $\delta(x)$ is finite by (3). Thus there exists some pair $(\hat{x}, \hat{g})$ such that $\hat{x} \in X^{\pm 1}$, $\hat{g} \in \delta(\hat{x})$, and, subject to those two constraints, $X\text{-length}(\hat{g}\hat{x})$ is as large as possible. By (4), $\hat{g} \in \delta(\hat{x})$ means $\hat{g} \neq 1$, $\hat{g}\hat{x} \neq 1$ and $\chi(\hat{g}) \neq \chi(\hat{g}\hat{x})$; by (4), this means $\hat{g}\hat{x} \in \delta(\hat{x}^{-1})$. Thus $X\text{-length}(\hat{g}\hat{x}) > X\text{-length}(\hat{g})$ by the maximality of $X\text{-length}(\hat{g}\hat{x})$.

Let $x_\dagger$ denote the element of $X^{\pm 1}$ such that $X\text{-length}(\hat{g}x_\dagger) < X\text{-length}(\hat{g})$. It suffices to show that $x_\dagger$ is a cutvertex of Γ. Notice that $x_\dagger \neq \hat{x}$. Now $X^{0,\pm 1}-\{x_\dagger\}$ equals the union of two disjoint nonempty subsets X_1 and X_2 with $\chi(\hat{g}X_1) = \{\chi(\hat{g})\}$ and $\chi(\hat{g}X_2) = \{\chi(\hat{g}\hat{x})\}$; here $1 \in X_1$ and $\hat{x} \in X_2$.

We next prove that

(5) no X-turn of $H_1 \cup H_2$ meets both X_1 and X_2.

Consider an arbitrary $h \in H_1 \cup H_2$. Let $(x_1, x_2, \ldots, x_n)$ be the shortest $X^{\pm 1}$-word for h. Set $x_0 := x_{n+1} := 1$. Each X-turn of h equals (x_i^{-1}, x_{i+1}) for some $i \in \{0, 1, \ldots, n\}$, and to prove (5) it suffices to show that (x_i^{-1}, x_{i+1}) does not meet both X_1 and X_2. We may assume that $x_\dagger \notin \{x_i^{-1}, x_{i+1}\}$, and it then suffices to show that $\chi(\hat{g}x_i^{-1}) = \chi(\hat{g}x_{i+1})$. Set $h' := x_i^{-1} x_{i-1}^{-1} \cdots x_1^{-1}$ and $h'' := x_{i+1} x_{i+2} \cdots x_n$. It suffices to show that $\chi(\hat{g}x_i^{-1}) = \chi(\hat{g}h') = \chi(\hat{g}h'') = \chi(\hat{g}x_{i+1})$.

We first show that $\hat{g}h'' \neq 1$ and $\chi(\hat{g}h'') = \chi(\hat{g}x_{i+1})$. If $i = n$, then $h'' = x_{n+1} x_{n+2} \cdots x_n = 1$ while $x_{i+1} = x_{n+1} = 1$. The case where $i = n$ is now clear. If $i \neq n$, then $x_{i+1} \in X^{\pm 1} - \{x_\dagger\}$, and, hence,

$$X\text{-length}(\hat{g}) < X\text{-length}(\hat{g}x_{i+1}) < X\text{-length}(\hat{g}x_{i+1}x_{i+2}) < \cdots < X\text{-length}(\hat{g}x_{i+1}x_{i+2}\cdots x_n).$$

By the maximality of X-length$(\hat{g}\hat{x})$, $\hat{g}x_{i+1} \notin \delta(x_{i+2})$. By (4), $\chi(\hat{g}x_{i+1}) = \chi(\hat{g}x_{i+1}x_{i+2})$. Continuing in this way, we see that

$$\chi(\hat{g}x_{i+1}) = \chi(\hat{g}x_{i+1}x_{i+2}) = \cdots = \chi(\hat{g}x_{i+1}x_{i+2}\cdots x_n).$$

Since $x_{i+1}x_{i+2}\cdots x_n = h''$, the case where $i \neq n$ is now clear also.

By using h' in place of h'' in the preceding argument, we see that $\hat{g}h' \neq 1$ and $\chi(\hat{g}h') = \chi(\hat{g}x_i^{-1})$.

By (3), $\delta(h) = \emptyset$. By (4), $\chi(\hat{g}h') = \chi(\hat{g}h'')$ since $(\hat{g}h')h = \hat{g}h''$. Thus, (5) holds.

Notice that X-turns$(R) \subseteq X$-turns$(H_1 \cup H_2)$, since each $r \in R$ equals-or-contains some $b \in H_1 \cup H_2$, whence X-turns$(r) \subseteq X$-turns$(\{b, b^2\})$. Since $\mathrm{E}\Gamma = X$-turns(R), it follows from (5) that no Γ-edge meets both X_1 and X_2. Since $X_2 \cup \{x_\dagger\} \subseteq X^{\pm 1} \subseteq \mathrm{V}\Gamma \subseteq X^{0,\pm 1}$, it suffices to show that $X_1 \cap \mathrm{V}\Gamma \neq \emptyset$. We may then assume that $\mathrm{V}\Gamma \neq X^{0,\pm 1}$, and here $\{y, y'\} - \{x_\dagger\} \subseteq X_1 \cap \mathrm{V}\Gamma$ by (2) and (5). This proves Theorem 5.1. □

5.2. The general cutvertex lemma. *If F is a finite-rank free group, R a finite subset of $\{g, {}^F g : g \in F - \{1\}\}$, and X an R-cutvertex-free F-basis, then $\underset{Y \in \mathcal{P}(X;R)}{*} \langle Y \rangle$ is an atomic R-allocating F-factorization.*

Proof. For each $Y \in \mathcal{P}(X;R)$, we know that $\mathcal{P}(Y; R_{|Y,X}) = \{Y\}$ and that $\mathbb{W}(Y, R_{|Y,X})$ has no Y-cutvertices; hence $\langle Y \rangle$ is an $R_{|Y,X}$-atom by Theorem 5.1. □

5.3. Whitehead's cutvertex lemma. *Let F be a finite-rank free group, B and X be F-bases, and R be a subset of B (resp. ${}^{\{F\}}B$). If X is R-cutvertex-free, then R is a subset of $X^{\pm 1}$ (resp. ${}^{\{F\}}(X^{\pm 1})$). Contrapositively, if R is not a subset of $X^{\pm 1}$ (resp. ${}^{\{F\}}(X^{\pm 1})$), then X is not R-cutvertex-free, whence $\mathbb{W}(X, R)$ has an X-cutvertex.*

Proof (Stong). This follows from Lemma 5.2 and Corollary 3.3. □

5.4. More notes on Whitehead's article. Each F-basis has only finitely many Whitehead neighbours. We say that X is *R-minimizing* if X'-length$(R) \geqslant X$-length(R) for each Whitehead neighbour X' of X. *Whitehead's minimizing algorithm* constructs, by trial and error, a Whitehead-neighbour-choosing sequence which starts at X, makes length(R) smaller with each step, and arrives at an R-minimizing F-basis in at most X-length$(R) - |R|$ steps. Whitehead's cutvertex algorithm, §4.6 above, shows that R-minimizing F-bases are R-cutvertex-free. The *only* fact highlighted by Whitehead(1936-01) was that his minimizing algorithm and his cutvertex lemma, when put together, constituted a sub-basis algorithm which could be applied to the study of three-manifolds. His cutvertex algorithm produces a faster sub-basis algorithm that is somewhat overlooked, perhaps because Whitehead(1936-10, Theorem 3) later proved an extremely useful result about R-minimizing F-bases. (Although stated for the case where $R \subseteq F$ or $R \subseteq {}^{\{F\}}F$, the result was proved for the case where $R \subseteq F \cup {}^{\{F\}}F$; see, for example, Dicks(2017).) If matches had been invented after the cigarette lighter, they would have been the sensation of the twentieth century, and if Whitehead had written (1936-01) after (1936-10), his cutvertex algorithm would have become the gold standard of sub-basis algorithms.

The marvellous *Quote Investigator* gives several published variants of the assertion about matches; the earliest one is attributed to Charles Norris. `https://quoteinvestigator.com/2017/12/06/matches/` □

References

E. Artin: Das freie Produkte von Gruppen. pp. 361–364 in Felix Klein: Vorlesungen über höhere Geometrie. Dritte Auflage. Bearbeitet und herausgegeben von W. Blaschke. Grundlehren Math. Wiss. **22**. Springer, Berlin, viii+405 pages (1926).

Warren Dicks: On free-group algorithms that sandwich a subgroup between free-product factors. J. Group Theory **17**, 13–28 (2014).

Warren Dicks: A graph-theoretic proof for Whitehead's second free-group algorithm. 14 pages (2017). `https://arxiv.org/abs/1706.09679`

S. M. Gersten: On Whitehead's algorithm. Bull. Amer. Math. Soc. **10**, 281–284 (1984).

Michael Heusener and Richard Weidmann: A remark on Whitehead's cut-vertex lemma. J. Group Theory **22**, 15–21 (2019).

A. H. M. Hoare: On automorphisms of free groups I. J. London Math. Soc. (2) **38**, 277–285 (1988).

A. Howard M. Hoare, Abraham Karrass, and Donald Solitar: Subgroups of finite index of Fuchsian groups. Math. Z. **120**, 289–298 (1971).

Alexander Kurosch: Die Untergruppen der freien Produkte von beliebigen Gruppen. Math. Ann. **109**, 647–660 (1934).

Herbert C. Lyon: Incompressible surfaces in the boundary of a handlebody – an algorithm. Canadian J. of Math. **32**, 590–595 (1980).

Reiner Martin: Non-uniquely ergodic foliations of thin type, measured currents and automorphisms of free groups. PhD thesis, UCLA, xi+87 pages (1995). `https://search.proquest.com/docview/304185823`

J. Nielsen: Om Regning med ikke-kommutative Faktorer og dens Anvendelse i Gruppeteorien. Mat. Tidsskrift B **107**, 77–94 (1921).

Jean-Pierre Serre: Arbres, amalgames, SL₂. Cours au Collège de France rédigé avec la collaboration de Hyman Bass. Astérisque **46**. Soc. Math. de France, Paris, 189 pages (1977).

Abe Shenitzer: Decomposition of a group with a single defining relation into a free product. Proc. Amer. Math. Soc. **6**, 273–279 (1955).

John R. Stallings: Whitehead graphs on handlebodies. pp. 317–330 in Geometric group theory down under (Canberra, 1996) (eds. John Cossey, Charles F. Miller III, Walter D. Neumann, and Michael Shapiro), Walter de Gruyter, Berlin, xii+333 pages (1999).

Edith Nelson Starr: Curves in handlebodies. PhD thesis, UC Berkeley, iv+22 pages (1992). `https://search.proquest.com/docview/303991902`

Richard Stong: Diskbusting elements of the free group. Math. Res. Lett. **4**, 201–210 (1997).

J. H. C. Whitehead: On certain sets of elements in a free group. Proc. London Math. Soc. (2) **41**, 48–56 (1936-01).

J. H. C. Whitehead: On equivalent sets of elements in a free group. Ann. of Math. (2) **37**, 782–800 (1936-10).

Henry Wilton: Essential surfaces in graph pairs. J. Amer. Math. Soc. **31**, 893–919 (2018).

Ying-Qing Wu: Incompressible surfaces and Dehn surgery on 1-bridge knots in handlebodies. Math. Proc. Cambridge Philos. Soc. **120**, 687–696 (1996).

Departament de Matemàtiques,
Universitat Autònoma de Barcelona,
E-08193 Bellaterra (Barcelona), SPAIN

Email address: `dicks@mat.uab.cat`
Home page: `http://mat.uab.cat/~dicks/`